REMARKS

Claims 1-22 are pending in this application.

In the Final Office Action, claims 1-8, 10-18 and 20-21 were rejected under 35 U.S.C. § 103 as being unpatentable over Hocker (U.S. 5,930,368, previously cited) in view of Muratov (U.S. 7,159,120, which is newly cited in the Final Office Action). In addition, claim 9 was rejected over Hocker in view of Muratov and further in view of Lygas, and claims 19 and 22 were rejected over Hocker in view of Muratov and further in view of Iijima (U.S. 4,800,520). All of these obviousness rejections are traversed. Applicants hereby request reconsideration of the rejections set forth in the Final Office Action in view of the following remarks, which establish that the Final Office Action fails to make out a proper showing of obviousness under 35 U.S.C. § 103 and the Supreme Court's holding in *KSR International Co. v. Teleflex, Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007).

In rejecting independent claims 1 and 12, the Final Office Action relies primarily on the Hocker reference, as in the prior office action, but now admits that Hocker "*does not expressly teach wherein the one or more security functions include deleting confidential information from a memory of the mobile device.*" (Final Office Action at page 3). It is important to note that this admittedly-missing function from Hocker occurs in claims 1 and 12 when the mobile device is stored in the mobile device holder. In an attempt to make up for this missing teaching from Hocker, the Final Office Action turns to Muratov, which teaches that data may be erased from the memory of a portable device, but only in two very limited circumstances. First, Muratov teaches that data may be erased from the mobile device after a "predetermined limited number of [faulty] attempts"[1] to access the data are detected by the portable device, such as, for example,

[1] Muratov, col. 2, line 5.

"after a predetermined number of non-valid passwords are entered that fail to match a valid password." (Muratov, col. 2, ll. 56-57). And second, Muratov teaches that data may be erased "after a predetermined time period between syncing the PDA to another device." (Muratov, col. 2, ll. 11-12).

Thus, even in combination, the references do not teach that confidential data is deleted from the memory of the mobile device when the mobile device is stored in the mobile device holder, as required in claims 1 and 12 of the present application. Hocker, admittedly, does not disclose erasing confidential data from the mobile device memory under any conditions, and Muratov only discloses erasing data when a faulty attempt to access the device is detected or when a predetermined time period has elapsed between data synchronization. Thus, the combination fails to disclose the subject matter of claims 1 and 12 and therefore the obviousness rejection should be withdrawn.

Furthermore, even if the combination of Hocker and Muratov disclosed all of the elements and limitations of claims 1 and 12, the Final Office Action fails to articulate any reasonable basis for combining the references that is not based on hindsight reconstruction of the applicants' claims. At page 3 of the Final Office Action, the stated conclusion of obviousness based on the combination of Hocker and Muratov is justified by the statement that "[t]he motivation for doing so would have been to provide additional security functions to maintain security of data/information stored on the mobile device."

First, this justification doesn't make any technical sense at all. In Hocker an address identifier or an encryption key is automatically exchanged between a portable device and a selected intelligent device upon docking the portable device. (Hocker, col. 3, ll. 25-34) Once removed, the portable device can then use the encryption key to transfer encrypted data to the

selected intelligent device. If this functionality were combined with Muratov, according to the Examiner, then there would be no reason to transfer data to the selected intelligent device because it would have been erased when the user of Hocker's device stored it into its holder. Thus, from a technical perspective, the combination of references does not make any sense.

Second, this justification is exactly the type of "conclusory statement" that the Supreme Court warned about in the *KSR* decision. In *KSR*, the Supreme Court stated that "[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." (*KSR*, 550 US ___, 82 USPQ2d at 1396). Here, there is no "articulated reasoning" or "rational underpinning" to support the combination of Hocker and Muratov other than the mere conclusion that it would "provide additional security functions." Certainly this is insufficient justification to support the hindsight reconstruction of the applicants claims based on the selective teachings of these references--teachings which, as noted above, are technically incompatible with one another.

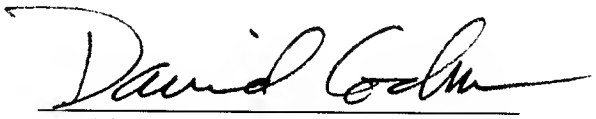
The rejection of claims 16 and 20 must also be withdrawn. In rejecting these claims, which add the limitation that the confidential information that is deleted from the memory of the mobile device is "a decrypted version of encrypted information," the Final Office Action relies upon the Hocker reference. This must be a mistake, however, because in rejecting the independent claims, the Final Office Action admitted that Hocker "*does not expressly teach wherein the one or more security functions include deleting confidential information from a memory of the mobile device.*" (Final Office Action at page 3). Thus, the Final Office Action's reliance upon Hocker for a further limitation of something that is admittedly missing from Hocker appears to be in error. Reconsideration is thus respectfully requested.

The rejection of claims 18 and 21 must also be withdrawn. In rejecting these claims, which add the limitation that the one or more security functions "include closing a data item currently being displayed," the Final Office Action admits that this limitation is missing from Hocker, but then erroneously relies upon Muratov. Specifically, the Final Office Action refers to column 2, ll. 36-38 and 53-57 of Muratov. These portions of Muratov, however, are silent with respect to "closing a data item currently being displayed." Rather, these portions of Muratov discuss the concept of "locking" the portable device once a number of faulty data access attempts are detected. Reconsideration is respectfully requested.

This application is now in condition for allowance.

Respectfully submitted,

JONES DAY



David B. Cochran (Reg. No. 39,142)
Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-7029